Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1375

Vragen van het lid **Alkaya** (SP) aan de Minister van Financiën over *het te grabbel gooien van onze bankgegevens door Brussel* (ingezonden 14 december 2018).

Antwoord van Minister **Hoekstra** (Financiën) (ontvangen 1 februari 2019). Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 1354.

Vraag 1
Kent u het bericht «De nieuwe Wehkamp»? Klopt de stelling dat zelfs de bankgegevens van mensen die geen toestemming hebben gegeven voor het delen daarvan in de database van een financieel-technologisch bedrijf terecht kunnen komen? Zo ja, kunt u dan aangeven hoe dit kan? Deelt u de mening dat dit voorkomen moet worden?[1]

Antwoord 1
Ja, ik ken het genoemde bericht uit De Groene Amsterdammer van 6 december 2018. Betaaldienstverleners kunnen in specifieke gevallen toegang krijgen tot gegevens van anderen dan de rekeninghouder. Dit kan bijvoorbeeld het geval zijn als de rekeninghouder toestemming heeft gegeven voor toegang tot zijn betaalrekening voor het maken van een huishoudboekje. Daarmee krijgt de betaaldienstverlener toegang tot betaalgegevens, maar alleen voor zover hij die nodig heeft voor het verlenen van de gevraagde betaaldienst. Die gegevens kunnen ook gegevens van derden omvatten, bijvoorbeeld als de rekeninghouder geld heeft overgemaakt aan een derde in een bepaalde periode. Dit betreft zogenoemde *silent party data*. De European Data Protection Board (EDPB) heeft eerder geoordeeld dat verwerking van *silent party data* door een betaalinitiatiedienstverlener of rekeninginformatiedienstverlener in het kader van PSD2 mogelijk is op grond van diens legitiem belang[2] bij uitvoering van het contract met de betaaldienstgebruiker (de rekeninghouder).[3] Daarbij wordt het legitiem belang beperkt en bepaald door de verwachtingen die een betrokkene redelijkerwijs mag hebben bij de verwerking van zijn gegevens. Daarom kunnen *silent party data* volgens de EDPB niet verwerkt worden voor andere doelen dan het uitvoeren van die specifieke betaaldienstovereenkomst.

---

[1] https://www.groene.nl/artikel/de-nieuwe-wehkamp
[2] Artikel 6(1)(f) AVG.
[3] https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf

ah-tk-20182019-1375
ISSN 0921 - 7398
's-Gravenhage 2019

Vraag 2
Waarom kunnen banken niet naar de rechter stappen als fintech-bedrijven data van hun klanten naar hun mening verkeerd gebruiken?

Antwoord 2
Als een bedrijf klantgegevens verkeerd gebruikt, kunnen zowel klanten zelf, banken als toezichthouders hiertegen stappen ondernemen, die uiteindelijk door een rechter kunnen worden getoetst. In de eerste plaats kan een klant het aan de Autoriteit Persoonsgegevens (AP) melden als een bedrijf naar zijn mening klantgegevens gebruikt in strijd met de Algemene Verordening Gegevensbescherming (AVG) of de daarop gebaseerde uitvoeringsregelgeving. De klant kan hierover ook een klacht indienen bij de AP. Daarnaast kan een bank een bedrijf de toegang tot de betaalrekening van de klant ontzeggen als zij aanwijzingen heeft dat het bedrijf niet-toegestane of frauduleuze toegang tot de betaalrekening heeft.[4] In dat geval moet de bank het incident ook onmiddellijk aan de Nederlandsche Bank (DNB) melden. DNB kan daarop zo nodig maatregelen nemen. Als DNB of de Autoriteit Financiële Markten (AFM) signaleren dat een bedrijf mogelijk klantgegevens verkeerd gebruikt, kunnen zij dit doorgeven aan de AP. De AP kan hierop vervolgens actie ondernemen. Bij het antwoord op vraag 3 wordt nader ingegaan op de mogelijkheden voor de AP en de betrokkene om naar de rechter te gaan. Bij het antwoord op vraag 4 wordt ingegaan op de mogelijkheden voor bedrijven om naar de rechter te gaan.

Vraag 3
Is de Autoriteit Persoonsgegevens, die toezicht moet houden op de fintech-bedrijven, wel in staat naar de rechter te stappen als data verkeerd worden gebruikt, al dan niet naar aanleiding van een signaal van een bank?

Antwoord 3
Op grond van de AVG kan een betrokkene die van mening is dat zijn gegevens onrechtmatig worden gebruikt daartegen een klacht indienen bij de AP. Als de AP oordeelt dat de persoonsgegevens inderdaad onrechtmatig worden verwerkt, kan zij als toezichthouder zelf handhavend optreden en maatregelen treffen, bijvoorbeeld een boete opleggen. De AP hoeft daarvoor niet naar de rechter. Een betrokkene heeft vervolgens de mogelijkheid om in beroep te gaan bij de bestuursrechter als hij het niet eens is met de wijze waarop de AP zijn klacht heeft afgedaan. Ook kan de betrokkene naar de civiele rechter om schadevergoeding te vorderen als de AP heeft geoordeeld dat er inderdaad sprake is van onrechtmatige gegevensverwerking.

Vraag 4
Kunnen fintech-bedrijven hun concurrenten of zakenpartners die privacyregels schenden wél juridisch aanspreken op misbruik? Kun u uw antwoord toelichten?

Antwoord 4
Een betrokkene heeft de mogelijkheid om een klacht in te dienen bij de toezichthouder (in Nederland de AP), als hij van mening is dat de verwerking van *zijn* persoonsgegevens in strijd is met de AVG. Bij (Fintech-)bedrijven die van mening zijn dat hun concurrenten of zakenpartners in strijd met de AVG handelen, zal hiervan geen sprake zijn. In zijn algemeenheid geldt dat als een bedrijf stelt schade te lijden als gevolg van onrechtmatig handelen van een ander bedrijf, het daartegen een procedure kan starten bij de civiele rechter. Tevens kan eenieder, dus ook een Fintech-bedrijf, bij de AP een signaal afgeven over mogelijk verkeerd gebruik van persoonsgegevens. De AP beziet vervolgens of zij hieromtrent een onderzoek instelt.

Vraag 5
Deelt u de mening dat PSD 2, de herziene betaaldienstenrichtlijn, is ingevoerd om kleine, innovatieve finanancieel-technologische bedrijven te helpen, maar uiteindelijk vooral de concurrentiepositie van de grote techbedrijven lijkt te versterken?

---

[4] Artikel 68(5) PSD2 en artikel 7:523 lid 5 BW.

Antwoord 5
Een doelstelling van PSD2 is het stimuleren en faciliteren van concurrentie en innovatie in de betaaldienstverlening. PSD2 creëert daartoe mogelijkheden voor toetreding van nieuwe partijen en een gelijk speelveld voor bestaande en nieuwe partijen op de Europese betaalmarkt. Alle partijen die betaaldiensten aanbieden op de Europese markt, of dat nu banken zijn, FinTech start-ups of grote technologiebedrijven, moeten voldoen aan dezelfde nieuwe PSD2 regels. Alle partijen moeten in het bezit zijn van een vergunning en staan onder permanent toezicht.
Ik begrijp de zorgen over de gevolgen van PSD2 voor de concurrentiepositie van grote techbedrijven op de Europese betaalmarkt. Om die reden heb ik tijdens de kamerbehandeling van het wetsvoorstel ter implementatie van PSD2 toegezegd deze ontwikkeling te zullen monitoren. Dit wordt uitgevoerd in nauwe samenwerking met de Autoriteit Consument en Markt. Ik informeer u in het voorjaar over de stand van zaken met betrekking tot de uitvoering van deze en andere toezeggingen die ik heb gedaan in het plenaire debat over PSD2.

Vraag 6
Herkent u het beeld dat er een omkering van bewijslast ontstaat bij misbruik van data zoals betaalgegevens, bijvoorbeeld wanneer een verzekeraar op basis van die data iemand in een bepaalde risicocategorie plaatst? Deelt u de mening dat de consument hierdoor in een onmogelijke positie komt, en dat dit uiterst onwenselijk zou zijn?

Antwoord 6
Het gebruik van betaalgegevens voor het maken van een risico-inschatting door een verzekeraar valt buiten de reikwijdte van PSD2. Gegevens van derden die daarvoor geen toestemming hebben gegeven – zogenoemde *silent party data* – mogen niet voor risico-inschatting worden gebruikt, omdat dit een ander doel is dan het uitvoeren van de betaaldienstovereenkomst is (zie ook antwoord op vraag 1). De kern van het verzekeringsbedrijf is het op basis van informatie over verzekerden een risico-inschatting maken en op basis daarvan een premie berekenen. Het is daarbij noodzakelijk om gebruik te maken van (persoonlijke) data.[5] Deze persoonlijke data kunnen ook betaalgegevens omvatten, mits daarvoor een rechtsgrond aanwezig is, zoals toestemming van de betrokkene. Het geven van toestemming moet voldoen aan een aantal eisen, waaronder dat toestemming vrijelijk moet zijn gegeven. Volgens de AVG is daaraan niet voldaan als betrokkene geen echte vrije keuze heeft of zijn toestemming niet kan weigeren zonder nadelige gevolgen.[6] De AP houdt toezicht op de naleving van deze eisen en kan zo nodig handhavend optreden. Daarnaast moet gewaakt worden voor onverzekerbaarheid voor hoge risico's. Het Verbond van Verzekeraars heeft de Solidariteitsmonitor geïntroduceerd. Daarmee wordt voor een grote en zeer diverse groep maatmensen doorgerekend hoe de premies zich ontwikkelen. Hiermee wil het Verbond de vinger aan de pols houden. Ik vind dit een goed initiatief. Op dit moment zijn er daarmee waarborgen om het gevaar van «omkering van bewijslast» bij gebruik van betaalgegevens tegen te gaan. Dit risico vergt blijvende aandacht van verzekeraars.

[5] Voor arbeidsongeschiktheids- en levensverzekeringen gelden in bepaalde gevallen, naast de AVG en UAVG, aanvullende regels. Deze staan in de Wet op de medische keuringen en zijn uitgewerkt in het Protocol Verzekeringskeuringen van het Verbond van Verzekeraars.
[6] Overweging 42 AVG.